DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 2/3/10 has been entered.

Response to Arguments

2. Applicant's arguments with respect to claim 2/3/10 have been considered but are moot in view of the new ground(s) of rejection.

The previously sited disclosure of 3GPP TS 33.220 v6.0.0 (2004-03) Generic Authentication Architecture (GAA); Generic Bootstrapping architecture March 2004, {herein after referred to as 3GPP} discloses the same features as the applicant's invention including a Bootstrapping Server Function see (BSF- Bootstrapping Server Function in fig. 1 page 7 of 3GPP; an application server see Network Application Function (NAF) in fig. 1 and section 4.2.2 on page 8; and Bootstrapping Transaction Identifier (B-TID) see ("Transaction Identifier" in section 4.3.7). Furthermore, 3GPP discloses Generic Authentication Architecture see (GAA in section 4.3.5 on page 9 and title) including the 3GPP Authentication Centre (see section 4 top on page 7).

The primary difference alleged by the applicant in independent claim 1 is that the application server function is in a visited network. In other words, the applicant's invention relates to the Bootstrapping Architecture of 3GPP with the further application of use with a visited network. Otherwise the 3GPP and the applicant's alleged invention are replete with the exact same concepts and features and functions. However, 3GPP clearly discloses "The architecture shall not preclude the support of network application function in the visited network, or possibly even a third network" in section 4.3 on page 8). The applicant's invention appears only to modify the prior art teaching of 3GPP in that applies to an application server in a visiting network and the feature of how to communicate with an application server in a visiting network is already widely known and used and would already be expected based on the disclosure of 3GPP in section 4.3

Specifically, Huotari et al. specifically discloses the application server in a visited network (see [0006] application server (AS) 60 may be located in an external or visited network, wherein further the services are provided to UE 40).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Huotari with that of 3GPP. Doing so would be necessary for users to obtain service-specific configurations upon registration such as Push to Talk over Cellular (See Huotari [0015]).

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 18-19 recites the limitation "A System" in relation to the claimed invention. Claims 18-19 are dependent from claims 16-17 which both are directed to an "Application Server" and do not mention or provide antecedent basis for "A system". There is insufficient antecedent basis for this limitation in the claims 18-19.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1, 5, 7, 10, 13, 16-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over 3GPP TS 33.220 v6.0.0 (2004-03) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping architecture (Release 6) 22

March 2004, pages 1-18 (XP002422872) {herein after referred to as 3GPP} in view of Huotari et al. (US 2004/0205212).

In regards to claim 1, 3GPP discloses A method for a roaming user (see "roaming subscriber",, 4.3.3 on page 9) to establish a security association with an application server (see Network Application Function NAF in fig. 1 and 4.2.1), comprising the steps of:

the application server receiving a service request from the roaming user (see "request" in fig. 2, page 11 & "application request" fig. 5, page 14 & pg. 10 section 4.4.2 in regards to UA interface "UE to request from ...NAF"), said service request message containing a Bootstrapping-Transaction Identifier (B-TID) (see section 4.3.7 "Transaction Identifier", Transaction Identifier used to bind the subscriber identity to the keying material in Ua" wherein see 4.4.2 UA is mechanism of service request from NAF), the B-TID being assigned to the roaming user by a Bootstrapping Server Function (BSF) based upon a mutual authentication of the roaming user with the BSF (see "mutual authentication between the UE and the BSF", see Sec. 4.4.1 page 10) that performs user identity initial verification in a generic authentication architecture in a home network of the roaming user (see section 4.4.3 "BSF to fetch the required authentication information and subscriber profile information");

the application server inquiring from an authentication entity in the about the roaming user's user information associated with the B-TID (see "authentication request TIdentifier" step 3 in fig. 5 on page 14), the user information comprising user authentication results of the generic authentication architecture in the roaming user's home network (see "authentication answer" for authentication results in page 14 fig. 5);

the authentication entity (see 3GPP Authentication Centre, section 4, page 7) finding out the home network to which the user belongs according to the B-TID (see section 4.3.7, "detect the home network and the BSF of the UE from the Transaction Identifier");

the authentication entity acquiring the user information associated with the B-TID from the BSF in the roaming user's home network (see two way exchange between BSF and HSS in fig. 3, page 3), and returning the acquired user information to the application server (see BSF supplies NAF the requested Key material, page 13 last paragraph);

the application server in the visited network obtaining the roaming user's user information comprising the user authentication results of the generic authentication architecture in the roaming user's home network (see section 4.3.5, "subscribers GAA profile information sent to BSF" wherein the BSF sends the profile information to the NAF", see section 4.3.6 page 9 "NAF shall be able to get the subscriber profile information needed for security purposes from the BSF"); and

the application server establishing a security association with the roaming user, according to the user authentication results of the generic authentication architecture in the roaming user's home network (again see 4.3.6 page 9 "NAF shall be able to get the subscriber profile information needed for security purposes from the BSF" and see step 4, application answer to UE in fig. 5 for further proof).

3GPP does not disclose the application server in a visited network. (In 3GPP the application server is in the home network, **however 3GPP clearly states "The architecture shall not preclude the support of network application function in the visited network, or possibly even a third network" in section 4.3 on page 8**). The applicant's invention appears only to modify the prior art teaching of 3GPP in that applies to an application server in a visiting network and the feature of how to communicate with an application server in a visiting network is already widely known and used and would already be expected based on the disclosure of 3GPP in section 4.3

Specifically, Huotari et al. specifically discloses the application server in a visited network (see [0006] application server (AS) 60 may be located in an external or visited network, wherein further the services are provided to UE 40).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Huotari with that of 3GPP. Doing so would be necessary for users to obtain service-specific configurations upon registration such as Push to Talk over Cellular (See Huotari [0015]).

In regards to claim 16, 3GPP discloses application server in a communication network comprising a home network of a roaming user (see "roaming subscriber",, 4.3.3 on page 9), comprising:

circuitry adapted for receiving a service request message see "request" in fig. 2, page 11 & "application request" fig. 5, page 14 & pg. 10 section 4.4.2 in regards to UA interface "UE to request from ...NAF") from the roaming user containing a Bootstrapping-Transaction Identifier (B-TID) (see section 4.3.7 "Transaction Identifier") , the B-TID being assigned to the roaming user by a Bootstrapping Server Function (BSF) based upon a mutual authentication of the roaming user with the BSF (see "mutual authentication between the UE and the BSF", see Sec. 4.4.1 page 10) that performs user identity initial verification in a generic authentication architecture in the home network of the roaming user (see "authenticate the subscriber by defining a Generic Bootstrapping Architecture", section 4 page 7);

circuitry adapted for inquiring from an authentication entity about an authentication to obtain the roaming user's user information associated with the B-TID (see section 4.4.3 Zn interface "fetch subscriber profile information from the BSF", & see section 4.5.3 near bottom "NAF starts communication over Zn interface comm" & "NAF requests key material corresponding to Transaction Identifier"); the roaming user's user information comprising user authentication results of the generic authentication architecture in the roaming user's home network (see section 4.3.5, page 9, "HSS shall be able to send subscribers GAA profile information needed for security purposes" and see authentication request and answer in steps 2-3 of fig. 5);

circuitry adapted for obtaining the roaming user's user information from the authentication entity after the authentication entity finds out the home network to which the user belongs according to the B-TID (see section 4.3.7 "detect the home network and BSF of the UE from the transaction Identifier" & see 4.5.4 "location information shall be discovered") and acquires the user information associated with the B-TID from the BSF in the roaming user's home network (see section 4.3.7 "detect the home network and BSF of the UE from the transaction Identifier); and

circuitry adapted for establishing a security association with the roaming user according to the user authentication results (see fig. 5 "Authentication Request" based on "TIdentifer" and Authentication Answer) of the generic authentication architecture in the roaming user's home network (again see "GAA Profile information" in section 4.3.5).

3GPP does not specifically disclose an application server in a communication network comprising a home network and visited network. 3GPP does not specifically disclose circuitry adapted for inquiring from an authentication entity about an authentication in the visited network. (However, see aforementioned claim 1, such concepts are notoriously well known and there use would be obvious to one in the art).

Huotari specifically discloses an application server in a communication network comprising a home network and visited network and circuitry adapted for inquiring from an authentication entity about an authentication in the visited network. (see [0006] application server (AS) 60 may be located in an external or visited network, wherein further the services are provided to UE 40, further see "registration and service control" with visited network AS, which includes auth. In [0006]).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Huotari with that of 3GPP. Doing so would be necessary for users to obtain service-specific configurations upon registration such as Push to Talk over Cellular (See Huotari [0015]).

In regards to Claim 5, 3GPP discloses acquiring the user information associated with the B-TID from the home BSF in the roaming user's home network (see Transaction Identifier shall be used to bind the subscriber identity in section 4.3.7 and see section 4.3.3 and "roaming user" and "architecture shall not preclude the support of network application function in the visited network" in section 4.3) .

However 3GPP does not specifically disclose wherein, the authentication entity in the visited network is an authentication, authorization and accounting (AAA) server in the visited network

Faccin discloses a AAA server in the home network inquiring the a Subscriber Database in the in the local network (see AAA server in home network, Fig. 2-4), after the Database in the local network finding the user information associated with the ("identifying information",

[0011]), it returning a response message, with the user information associated with the (identifying information [0011]) in it, to the local AAA server , and the AAA server returning a response message , with the user information associated with the (identifying information [0011]) in it, to the AAA server in the visited network (see AAA server in the visited network); the AAA server in the visited network obtaining the user information associated with the (see final results H-GW sent to AAA in fig. 4) from the response message returned by the AAA server in the roaming user's home network (page 3, line 15-page 4, line 1 ;page 6, lines 16-23; page 8, lines 13-20; page 10, line 9-page 11, line 1; figure 2;claim 4).

It would have been obvious to one of ordinary skill in the art at the time of the invention, namely when the same result is to be achieved (see page 8, lines 27-28 of document 3GPP; page 2, lines 9-23 of document Faccin), to apply the features disclosed by Faccin as they relate to identifying information/B-TID with corresponding effect to the method to establish security association according to document 3GPP in view of Huotari, thereby arriving at a method for a roaming user to establish a security association according to claim 1. The motivation for doing so would be allow mobile operators to operate/provide multiple secured networks multiple different organizations at once.

In regards to claims 7 & 17 3GPP in view of Huotari discloses the method according to Claim 1, wherein the user information comprises at least: key information and the user's identity (see section 4.2.2 & 4.2.4 “Key material” , “key identifier" in 4.3.7 and subscriber identity in section 4.3.7).

In regards to claim 10, 3GPP 3GPP in view of Huotari discloses the method according to Claim 7, wherein the user information also comprises the profile information associated with security (See GAA profile in section 4.3.5 and subscriber profile in section 4.3.6).

In regards to claim 13, 3GPP in view of Huotari discloses the method according to Claim 7, wherein the key information is a shared key Ks generated in authentication, or a Ks-derived key and its valid term (see number 8 on page 12 "keys shared between UE and any NAF“).

In regards to claim 18, 3GPP in view of Huotari discloses a system, comprising an application server according to any of claims 16-17, wherein the application server is connected with the authentication entity (see NAF and HSS via Zh and Zn interface in fig. 4.1), and the authentication entity comprises circuitry adapted for finding out a user's home network entity (see section 4.3.7 …. “detect the home network and BSF”)

In regards to claim 19, 3GPP in view of Huotari discloses the system according to Claim 18, wherein the authentication entity further comprises circuitry for communicating with a BSF (see BSF in fig. 4.1).

8. Claims 3-4 are rejected under 35 U.S.C. 103(a) as being unpatentable over 3GPP TS 33.220 v6.0.0 (2004-03) 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping architecture (Release 6) 22 March 2004, pages 1-18 (XP002422872) {herein after referred to as 3GPP} in view of Huotari et al. (US 2004/0205212) in further view of Faccin (US 2003/0033518 A1).

In regards to claim 3, 3GPP in view of Huotari discloses the method according to claim 1, wherein the authentication entity in the network is a BSF or a generic authentication architecture proxy (see BSF in fig. 1);

the step of the BSF or the generic authentication architecture proxy in the network acquiring the user information associated with the B-TID from the roaming user's home (see section 4.3.3 "roaming user shall be able to utilize bootstrapping function in the home network" page 9 & see section 4.3.7 "requirements on transaction identifier" … "NAF shall be able to detect the home network and the BSF of the UE from the transaction identifier",) network comprises:

the BSF or the generic authentication architecture proxy in the network directly sending a query message to the BSF in the roaming user's home network (see step 2 in fig. 3 wherein BSF obtains information form home network), inquiring about the user information associated with the B-TID (see "user profile"); and obtaining the user information associated with the B- TID from the response message returned by the BSF in the roaming user's home network (see "Transaction Identifier" obtained by BSF in fig. 5).

3GPP and Huotari do not specifically discloses the authentication entity in the visited network is a BSF or a generic authentication architecture proxy.

Faccin et al. specifically discloses disclose the authentication entity in the visited network is a BSF or a generic authentication architecture proxy (see AAA server in fig. 2).

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Fenton with that of 3GPP and Huotari. Doing so would be necessary to improve user mobility by utilizing the mobile IP protocol (See Fenton col. 1, lines 52-60)

In regards to claim 4, 3GPP in view of Huotari in further view of Fenton disclose the method according to Claim 3.

3GPP in view of Huotari does not disclose wherein the generic authentication architecture proxy in the visited network is an independent server, or a server combined with an authentication, authorization and accounting (AAA) server in the local network, or a server combined with the application server in the local network.

Faccin discloses disclose wherein the generic authentication architecture proxy in the visited network is an independent server (see standalone GW & AAA Server in fig. 2), or a server combined with an authentication, authorization and accounting (AAA) server in the local network (see AAA server in fig. 2), or a server combined with the application server in the local network.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the teachings of Fenton with that of 3GPP and Huotari. Doing so would be necessary to improve user mobility by utilizing the mobile IP protocol (See [0008] of Faccin).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KHALID SHAHEED whose telephone number is (571)270-5813. The examiner can normally be reached on Monday-Friday 8am-5pm; EST; ALT Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kamran Afshar can be reached on 571-272-7796. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/KHALID SHAHEED/

Examiner, Art Unit 2617

/KAMRAN AFSHAR/

Supervisory Patent Examiner, Art Unit 2617